Deception used for Cyber Defense of Control Systems

Miles A. McQueen†, Wayne F. Boyer†
†Idaho National Laboratory, Idaho Falls, Idaho, USA

Abstract — **Control system cyber security defense mechanisms may employ deception in human system interactions to make it more difficult for attackers to plan and execute successful attacks. These deceptive defense mechanisms are organized and initially explored according to a specific deception taxonomy and the seven abstract dimensions of security previously proposed as a framework for the cyber security of control systems.**

Keywords — **Control Systems, Cyber Security, Deception.**

I. Introduction

THE use of some forms of deception for defense against cyber attacks is common practice in computer security [1]. For example, a honeypot is a computer designed to attract attackers by impersonating another machine that may be worthy of being attacked. Encryption, for another example, is a common security measure that attempts to deceive by hiding information within a hopefully confusing string of seemingly random symbols. More generally, randomization is an important component of deception in computer security, because randomization could prevent attackers from gathering information that can be used to predict exploitable system behavior.

Unfortunately the role of deception is rarely explicitly acknowledged and thus opportunities for defensive deception may be missed. Our thesis is that there are currently unexplored deception mechanisms which could be used for control system cyber security defense that have the potential to make it more difficult for attackers to succeed. This paper represents an initial exploration of various types of deceptions as they relate to cyber security for control systems. The taxonomy of deception from Rowe and Rothstein [2] is used, in conjunction with the seven dimensions of control system cyber security proposed in our previous work [3], as a guide in the exploration of potential defensive mechanisms.

Work supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory.

II. Deception taxonomy

Deception is fundamentally about distorting an adversary's perceptions of reality. The distortion may be self-induced, may be accidental, or may be deliberate [4]. The first two possible causes of the misperception, self induced and accidental, are not addressed in this paper. The third possible cause for misperception, deliberate deception may be intended to aid the deceived but is relevant to the defense of control systems only when the deception is intended to put an adversary at a disadvantage. For example, the defender of a control system may have deployed a simple and cheap computer as a canary in order to detect if an attacker, the adversary, has penetrated into the system. This is the version of deception that is clearly applicable to the defense of control systems and will be used in the rest of this paper.

There is no one settled and agreed upon definition of deception. Some definitions are ethically neutral, others clearly aren't. A discussion of conceptualizations and definitions for deception may be found in many papers [5] [6]. In this paper we use the definition proposed by Burgoon et al [7]. Deception is "A deliberate act perpetrated by a sender to engender in a receiver beliefs contrary to what the sender believes is true to put the receiver at a disadvantage**".**

A variety of taxonomies have been proposed for deception. We will use the taxonomy proposed by Bell and Whaley [8]. Deception consists of dissimulation, hiding the real, and simulation, showing the false. Dissimulation consists of three potential techniques. The first technique is **masking** the real by making a relevant object be undetectable or blend into background irrelevance. For example, malicious JavaScript may be embedded as white space in relatively benign looking JavaScript [9], or a second important private text message may be embedded as white font in the white space of an apparently innocuous email message sent to a group. The second technique is **repackaging** which hides the real by making a relevant object appear to be something it isn't. For example, a phishing attack may make use of a very innocuous, official, or friendly looking subject line in order to entice a receiver to open the message; or an anonymizing remailer may be used to replace the actual sender identification information in an email message. The third dissimulation technique is **dazzling** which hides the real by making the relevant object identification be less certain by confusing the adversary about its true

nature. Methods for inducing confusion include randomization and obfuscation of identifying elements of the object. For example, an encrypted channel makes use of obfuscation to hide the meaning of the message even though it is still clear a message was sent.

Simulation, displaying the false, also consists of three potential techniques. The first simulation technique is **inventing** the false by creating a perception that a relevant object exists when it doesn't. For example, a honeypot may be used to give the appearance of a subnet of machines with specific IP addresses when in fact there is no such subnet. The second simulation technique is **mimicking** which invents the false by presenting characteristics of an actual, and relevant, object. For example, a phishing attack may link to a web page that appears to be the valid web page of a reputable firm e.g. bank of America, but is in fact a malicious web page created by the phisher. The third simulation technique is **decoying** which displays the false by attracting attention away from more relevant objects. For example, providing a web page with false but believable data on critical infrastructure systems may be used to attract an adversary's attention away from sources of real data.

In every deception there is both simulation and dissimulation, whether explicit or implicit. Inherently hiding the real must also involve some form of displaying the false. Using the taxonomy of dissimulation and simulation, this paper will explore, within a cyber security framework, the use of deceptive mechanisms which may be used by defenders of critical control systems to aid in protecting the system from damaging cyber attacks.

TABLE 1. SEVEN ABSTRACT DIMENSIONS OF SECURITY AND ASSOCIATED IDEALS

Security Dimension	***Ideal***
1. Security Group (SG) knowledge	1. Security Group (SG) knows current control system perfectly
2. Attack Group (AG) knowledge	2. Attack Group (AG) knows nothing about the control system
3. Access	3. The control system is inaccessible to AGs
4. Vulnerabilities	4. The control system has no vulnerabilities
5. Damage potential	5. The control system cannot cause damage
6. Detection	6. SG detects any attack instantly
7. Recovery	7. SG can restore control system integrity instantly

III. CONTROL SYSTEM CYBER SECURITY FRAMEWORK

The control system cyber security framework consists of seven security dimensions and provides the foundation for defensive actions. Each of the seven dimensions of security represents an important aspect of the control system's security posture at a given point in time. Each dimension has an associated ideal that represents perfection for that aspect of security. The seven dimensions of security are listed in Table 1 each with its associated ideal and then discussed more fully in the rest of this section.

A. Security Group Knowledge

The first control system security dimension is Security Group (SG) knowledge. The security group represents those people who are directly responsible for the security of the control systems. Security risk is strongly correlated with the security group's knowledge of the system. In the ideal situation, the security group has perfect knowledge of the system including all the hardware and software components, network topology, communication paths, normal operational behavior, and even vulnerabilities. That knowledge is needed for the security group to effectively make security decisions that protect the control system from potential attackers. Any changes that occur to the control systems without the security group's knowledge may inadvertently introduce new vulnerabilities into the system and inhibit the introduction of reasonable mitigation measures. Perfect knowledge of the system implies a configuration management process that includes the security group in the planning of all changes and provides a mechanism for alerting the security group to any unauthorized changes.

B. Attack Group Knowledge

The second control system security dimension is Attack Group (AG) knowledge. The attack group represents any of the many potential adversaries in the world who might have interest in attacking through cyber means. Security risk from targeted attacks is kept down when potential attackers are unable to obtain any information about the control system. Ideally, anyone who is not authorized to use the control system should be prevented from gaining knowledge of its design or configuration and be unable to obtain any information that would allow them to plan and execute an attack. This includes information an attacker might gain about the control system after they have compromised portions of it and information they might gain from other sources before the attack commences (e.g., a vendor's web site touting a specific facility as a success story).

It is important to recognize that even approved users may become members of an attack group when their actions on the system go beyond what they are authorized to perform, whether inadvertently or intentionally (the "insider threat").

Kerckhoffs' principle was stated by Auguste Kerckhoffs in the 19th century: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. [10] This principle has been used to argue against dependence on "security through obscurity". Bruce Schneier suggests that "Kerckhoffs's principle applies beyond codes and ciphers to security systems in general." [11] This principle emphasizes that defenses

should not rely on only one dimension of security (Attack Group Knowledge). We also assert that although it is unwise for a defender to assume that an attacker cannot obtain design information on products such as encryption algorithms or protocols, the security of a specific installation is in fact better when attackers cannot obtain accurate knowledge of that installation and its defenses.

C. Access

The third control system security dimension is Access. Even though authentication mechanisms are designed to prevent unauthorized use of data transfer paths, the existence of every path, authenticated or not, negatively impacts security risk. The ideal situation from a security perspective is to disallow any communication channels between the control system and any location where there are potential attackers. Although achievement of this ideal is not practical in most cases, the ideal includes the absence of any electronic connections between the Internet and the control system.

D. Vulnerabilities

The fourth control system security dimension is Vulnerabilities. A vulnerability is any weakness or defect in the system that provides a potential attacker with a means to gain privilege intended for authorized users only. An exploit of a vulnerability leads to a compromise. An ideal system has no weaknesses and no defects. Unfortunately, all systems have weaknesses and if an attack group is targeting a specific control system facility they will be actively searching vulnerability disclosure sites and using techniques such as reverse engineering to find the weaknesses in that facility.

E. Damage Potential

The fifth control system security dimension is Damage Potential. The ideal control system cannot cause physical damage even if the electronic networks are completely compromised by an attacker. Since risk is the expected value of loss, the damage potential is directly proportional to risk. The amount of damage that can be caused by a compromised control system is determined by the type of process that it controls and by the nature of engineered safety systems (e.g., physical safety mechanisms may be in place that prevent significant damage despite a successful attack on the electronic control system).

A cyber attack also has the potential for non-physical damage in the form of information loss (e.g. loss of privacy, loss of valuable intellectual assets such as trade secrets or financial data). However, the data that may be stolen is generally not the end target of a control system attack but rather the physical process it controls.

F. Detection

The sixth control system security dimension is Detection. An ideal control system includes detection mechanisms that alert the Security Group whenever there is an unauthorized event on the control system. Unauthorized events come in a wide variety of forms and would include activities such as an unauthorized user attempting to gain access to the control system or a counterfeit message from a front end processor to a remote terminal unit (RTU).

G. Recovery

The seventh control system security dimension is Recovery. An ideal control system can be restored to an uncompromised state immediately after an attack is detected. Recovery time is related to Damage Potential because the cost of a successful attack correlates with the length of time that the control system is in a compromised state. Damage will tend to be less severe if the time to recover is minimized. However, the relationship between Recovery Time and Damage Potential is highly non-linear and highly system dependent.

For each of these seven dimensions of security there are deceptive mechanisms which in principle could be used to increase the defensive team's ability to defend the control system and facility from a cyber attack. A few potential deceptive mechanisms are explored in the next section with at least one suggested defensive mechanism for each dimension. Each defensive mechanism, independent of security dimension, is intended to deceive the attacker in some fashion and thus make the attack less effective.

IV. DECEPTIVE DEFENSE MECHANISMS

Defensive mechanisms for each of the six deception types are suggested for each of the seven dimensions of security. Deceptive defensive mechanisms are often applicable to multiple categories of deception and to multiple dimensions of security. For example, mechanisms that hide information from attackers apply to the Attack Group Knowledge dimension of security and can also be applied to other dimensions such as Security Group Knowledge and Vulnerabilities.

A. Security Group Knowledge

Processes and mechanisms that help the security group to know and manage their systems well, also improve security. Deception mechanisms that apply to this dimension of security would help to prevent attackers from defeating the processes that the security group uses to manage their systems. For example, randomizing system diagnostics and the timing of audits to reduce predictability could make it difficult for potential attackers to defeat those mechanisms. Table 2 lists a few potential defensive mechanisms that use deception to improve security in the "SG knowledge" dimension.

TABLE 2. DECEPTION DEFENSES FOR **SECURITY GROUP KNOWLEDGE** SECURITY DIMENSION

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide security group processes from attackers.*

Masking	Masking can be used to hide security group processes from attackers by making them invisible. • The security plan should be hidden from the view of any unauthorized personnel. • All communications and data associated with security group processes should be hidden, perhaps by steganography.
Repackaging	Repackaging hides security group processes by making them appear to be something that is of no interest to the attacker. • The security plan and configuration management plan could be hidden within a file that has an uninteresting name and location.
Dazzling	Dazzling can be used to hide security group processes by confusing with randomization. • Encrypt the security plan. • Randomize the time at which security tests and audits are performed.
Simulation	*Defenses that show false security group actions*
Inventing	Attackers could be confused by the creation of spurious information that describes security processes and policies that do not exist. • Fake documentation of non-existent security policies and procedures.
Mimicking	Mimicking deceives by imitating something of interest to the attacker. • Fake system logs. Fake logs could be erased or modified by the attacker, to cover his tracks, while the real system logs remain hidden.
Decoying	Decoying offers false information designed to divert the attacker's attention. • Spurious messages appearing to be from a honeypot.

B. Attack Group Knowledge

Attackers will be less successful, if they are unable to easily collect information about the control system that can be used for exploitation. Deception is particularly applicable to Attack Group Knowledge because deception is aimed at limiting the attacker's knowledge of actual reality and creating within the attacker a false perception of reality. The most common deception technique for this dimension of security is simple masking. That is, the prevention of information leaks. However, the deception techniques of repackaging, dazzling, inventing, mimicking and decoying can also be used to hide information and generate misinformation to confuse the attacker. For example, false network traffic that attackers are able to intercept may contain misleading data about how the system is designed and configured. Misleading the attacker would ideally include deceptions related to the other dimensions of security. Information about "Access", "Vulnerabilities" and "Damage Potential" can be hidden by deception and can also be made to appear much different to the attacker than they are in reality. Table 3 lists a few potential defensive mechanisms that use deception to improve security in the "AG knowledge" dimension.

TABLE 3. DECEPTION DEFENSES FOR **ATTACK GROUP KNOWLEDGE** SECURITY DIMENSION

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide information about the control system from attackers*
Masking	Masking includes all methods that prevent attackers from observing information about the system. • Configure to not answer pings. • Limit publication of information about the system. • Use switches not hubs to reduce sniffing potential. • Hide information within a cover medium, using stenography.
Repackaging	Repackaging hides system information by making it appear to be something that is of no interest to attackers. • Control system schematics and configuration information could be hidden within a file that has an uninteresting name and location.
Dazzling	Dazzling can be used to hide information about the system by making the information which may be observable to attackers be confusing or unintelligible. • Encryption should be used on all communication paths when feasible. • Any electronic file that contains information about the system

	should be protected by encryption.
Simulation	*Defenses that show false information about the control system to attackers*
Inventing	Invention is intended to create the perception that the system includes components and functions that in reality do not exist. • Phony System schematics and other documentation that can be downloaded from a web site or FTP site. • Fake, plain text, message traffic appearing to be to and from a shadow control room which doesn't exist.
Mimicking	Mimicking can deceive the attacker into perceiving that an unimportant part of the system is important and relevant to their attack. • Phony machines (perhaps virtual machines) could be connected to the control system network and be made to mimic machines that are attractive attack targets such as Remote Terminal Units (RTU) controlling critical portions of the system or Human Machine Interface (HMI) computers.
Decoying	Decoying is a diversion meant to divert the attacker's attention away from critical targets. • False but seemingly important HMI commands which draw attention to relatively benign portions of the system.

C. Access

From a security perspective, the number of accessible services should be minimized. For services that are required, they can be protected by masking, repackaging (use an uninteresting service as a wrapper for sensitive communications), etc. Randomization of IP addresses, or ports, could be used for dazzling. Many open ports that lead to nowhere and false traffic that implies access that does not exist could be used to confuse an attacker. Table 4 lists a few potential defensive mechanisms that use deception to improve security in the "Access" dimension.

TABLE 4. DECEPTION DEFENSES FOR **ACCESS** SECURITY DIMENSION

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide services from attackers*
Masking	Masking is any method that prevents attackers from observing services associated with the control system. • Configure to not answer pings. • Configure firewalls to prevent traffic flow between the control system and external networks except as required. • Hide control system communications from external networks behind a NAT (network address translation) device.
Repackaging	Repackaging hides service information by making the service appear to be something that is of no interest to attackers. • Running a service on a non standard port. • Providing service connect headers which make the service appear to be another, more secure, version of the same service e.g. make Wu-FTP appear to be ProFTP.
Dazzling	Dazzling can be used to hide information about the system services by making what is observable by attackers confusing or unintelligible. • Encryption should be used for all services when feasible. • Randomization of IP addresses.
Simulation	*Defenses that show false services*
Inventing	Inventing is any deception that causes the attacker to falsely observe services that do not exist. • False network traffic that contains IP addresses and ports that do not exist.
Mimicking	Mimicking can deceive the attacker into perceiving that a relatively unimportant service is a critical component of the control system. • If there are multiple versions of the same service, make them all appear to be the same version on the same machine.
Decoying	Decoying is a diversion meant to

	divert the attacker's attention away from critical aspects of the control system network. • False network traffic that leads the attacker to phony, seemingly vulnerable services located in virtual machines.

D. Vulnerabilities

The primary defensive mechanism in this dimension of security is the timely patching or other mitigations of known vulnerabilities e.g. make the vulnerability inaccessible. Dissimulation will apply techniques to make the vulnerabilities more difficult to discover e.g. give the appearance of being patched when the service hasn't been or e.g. randomize the system in some fashion to make the vulnerabilities dynamic and less likely to be discovered/exploited [12]. Simulation attempts to present to the attacker vulnerabilities which don't really exist e.g. give the appearance of an unpatched version of the service. Table 5 has these and a few other potential defensive mechanisms that use deception to improve security in the "Vulnerabilities" dimension.

TABLE 5. DECEPTION DEFENSES FOR **VULNERABILITIES** SECURITY DIMENSION

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide vulnerabilities from attackers*
Masking	Vulnerabilities are hidden by masking when they are made invisible to the attacker. • Firewalls that restrict access to only the required machines and services not only block access to vulnerabilities but also prevent the attacker from identifying them.
Repackaging	The vulnerabilities of a specific service will be hidden from an attacker when the attacker is deceived into believing that it doesn't exist. • Services which provide system unique banners unrelated to the actual service connected to the port may mask the existence of actual vulnerabilities in the service.
Dazzling	Vulnerabilities may be hidden by randomizing the behavior of the software that communicates with potential attackers. • Pucella and Schneider [12] described a framework for the obfuscation of software implementation details that makes it more difficult for attackers to predict exploitable behaviors.
Simulation	*Defenses that show false vulnerabilities*
Inventing	A deception that creates the impression that the control system has vulnerabilities that in fact do not exist. • Virtual machines with many fake services and associated vulnerabilities. • Network maps indicating accessibility to non existent machines and services with vulnerabilities.
Mimicking	Mimicking can deceive an attacker into attempting to exploit something that is not a significant part of the system. • A service that mimics the behavior of a common service but on a virtual machine whose compromise would cause little or no damage.
Decoying	Decoying is a diversion. • False traffic that leads attackers to fake virtual machines and therefore leads them away from real vulnerabilities.

E. Damage Potential

Security risk is reduced if there are mechanisms independent from the control system that reduce the amount of damage that can be done by a compromised control system. Misinformation which would lead attackers to believe that the potential damage is less than the true potential would also reduce the risk of an attack because that belief would make the target less attractive. Any other deception that confuses attackers such that their actions result in less damage to the system reduces security risk. Table 6 lists a few potential defensive mechanisms that use deception to improve security in the "Damage Potential" and "Recovery" dimension.

TABLE 6. DECEPTION DEFENSES FOR **DAMAGE POTENTIAL** AND **RECOVERY** SECURITY DIMENSIONS

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide damage potential from attackers.*
Masking	Masking makes the damage potential invisible. • Limit distribution/publication of information that describes

	the true damage potential. (explosions, release of toxic material, etc.)
Repackaging	Repackaging deception hides the true potential damage that could be caused by a subsystem or component by creating the appearance that the attackers actions using the subsystem will not cause significant damage. • Add incorrect information to the system physical safety documentation to create a publicly accessible false document to imply that the subsystem will fail safe.
Dazzling	Damage potential may be hidden by making the information related to damage potential confusing or unintelligible. • Damage potential information should be encrypted. • Use non standard symbols and labeling in system diagrams.
Simulation	*Defenses that show false damage potential*
Inventing	A deception that creates the impression that there is damage potential that does not exist in reality. • Fake system documentation about the physical plant that can be accessed by attackers through FTP or web sites. The documentation may show subsystems with great damage potential that don't in fact exist. (Note: This technique could have the unwanted consequence of increasing the attractiveness of the control system as a target).
Mimicking	Mimicking creates the appearance of more serious damage than the true result of an attacker's malicious action. • Fake system documentation about the physical plant that can be accessed by attackers through FTP or web sites. The documentation may show a subsystem without a physical safety device which in fact has the safety mechanism. (Note: This technique could have the unwanted consequence of increasing the attractiveness of the control system as a target).
Decoying	A diversion that leads attackers away from actions that would cause the most severe damage. • Fake network traffic with indicators that a relatively harmless portion of the system has high damage potential (e.g. an HFL tank).

F. Detection

Attackers will often need to remain undetected for relatively long periods of time in order to fully compromise and damage a control system and its facility. Consequently, detection is an important aspect of securing a system. Deception may be used to aid detection in a variety of ways. For example, honeypots may be used to attract attackers and therefore may be used to detect an attack in progress; an inexpensive canary may be set up such that any traffic to the machine triggers an alarm; false network traffic can lead an attacker into believing that a port or IP address on a honeypot is a valid target, but accessing that IP address and port causes an attack alarm. Table 7 lists a few defensive mechanisms that use deception to improve security in the "Detection" dimension.

TABLE 7. DECEPTION DEFENSES FOR **DETECTION** SECURITY DIMENSION

Type of Deception	***Defensive actions***
Dissimulation	*Defenses that hide detection mechanisms from attackers*
Masking	Masking makes the detection mechanisms invisible. • Limit publication of any information about the existence of detection mechanisms on the control system. • Intrusion detection mechanisms should not be detectable by an attacker who has compromised part of the system. For example, an anti-virus program should obfuscate its name and, as much as possible, other identifiable features.
Repackaging	Repackaging makes a detection mechanism appear to be something of no significance to the attacker. • A "canary" is a device that alarms whenever data is sent to it. Under normal operations no data is ever sent to that address. Add sophistication by making the canary appear to be a functioning and important part

	of the functional control system.
Dazzling	Techniques that obscure detection mechanism characteristics from the attacker by making them confusing or unintelligible. • Randomization. • Encrypt all information about actual detection mechanisms, and all traffic related to detection mechanisms.
Simulation	*Defenses that show false detection mechanisms*
Inventing	Techniques that create the impression that detection mechanisms exist that do not exist in reality. • Fake system documentation showing the installation of many detection mechanisms which don't exist. Make the document reasonably accessible to an attacker (e.g. install unencrypted on the engineering workstation).
Mimicking	Mimicking the functions of an intrusion or malware detector may scare the attacker away. • Fake intrusion alarms that are observable by an attacker but are ignored by operations.
Decoying	A diversion that leads attackers away from learning about detection mechanisms and toward a mechanism that detects the attack. • Fake network traffic that leads to virtual machines that appear to be attractive targets but are actually attack detectors.

G. Recovery

Recovery is closely related to damage potential. Faster recovery usually means less damage and less damage usually leads to easier recovery. Therefore, the same deceptive defense mechanisms that apply to damage potential also apply to recovery. See Table 6.

V. Complexity

The use of deception is related to control system complexity. Control systems are very complex. Increased complexity impacts the ability of the security group to understand and manage the system, therefore the first dimension of security is negatively impacted by complexity. Increased complexity of the network interfaces increases the likelihood of a defect, and defects lead to vulnerabilities potentially reachable and exploitable by an attacker. Complexity would seem to be the enemy of security.

But from an attacker's perspective, increased complexity along with incomplete or incorrect information is a mixed blessing. The control system complexity provides opportunity for the attacker but also creates added difficulty in understanding the system, remaining undetected, and determining the steps necessary to cause significant damage. The use of deception by the control system security group has the potential to make the attack complexity even greater for the attacker, and thus the attacker's goals would be more difficult to obtain. Deception can help turn complexity into an advantage for the defender.

VI. Conclusion

Some forms of deception for defense against cyber attacks are currently in use on enterprise systems. Recent research has begun to investigate more comprehensive application of deception. In control systems much less investigation of deception has occurred.

We have begun exploration into the possible role of deception in control system cyber security defenses by mapping a taxonomy of deception to seven dimensions of cyber security. We have identified opportunities for improved defense by the explicit use of deception. Several deceptive mechanisms of various types combined into a coordinated defensive strategy may provide the best approach. This preliminary exploration will be used to guide future studies of deception techniques for control systems and guide research into specific and detailed defensive mechanisms.

References

[1] J. Yuill, et. al., "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques", *Journal of Information Warfare*, 2006.

[2] N. Rowe, H. Rothstein. "Two Taxonomies of deception for Attacks on Information System, *Journal of Information Warfare*, 2004.

[3] W. F. Boyer, M. A. McQueen, "Ideal Based Cyber Security Technical Metrics for Control Systems", *CRITIS'07 2nd International Workshop on Critical Information Infrastructures Security*, October 3-5, 2007.

[4] B. Whaley, "Toward a general theory of deception", *The journal of Strategic Studies*, 178-192, 1982.

[5] J. Masip, E. Garrido, C. Herrero, "Defining Deception", Annals of Psychology, vol 20, June, 2004

[6] http://plato.stanford.edu/entries/lying-definition/

[7] J. K. Burgoon, D. B. Buller,"Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics", *Journal of Nonverbal Behavior*, vol. 18, pp. 155-184, 1994.

[8] J. Bell, B. Whaley, "Cheating and Deception", Transaction Publishers, New Brunswick, NJ, 1982.

[9] Kolisar, "WhiteSpace: A different Approach to JavaScript Obfuscation ", DEFCON 16, August 8, 2008

[10] Auguste Kerckhoffs, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.

[11] Mann, Charles C. (September 2002). "Homeland Insecurity". The Atlantic Monthly 290 (2).

[12] R. Pucella, F. B. Schneider, "Independence From Obfuscation: A Semantic Framework for Diversity", *Technical report, Cornell University, TR2006-2016*, January, 2006.